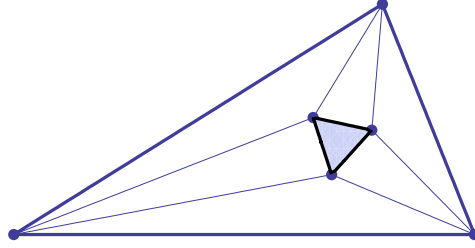


MORLEY'S OTHER MIRACLE: $4^{p-1} \equiv \pm \binom{p-1}{\frac{p-1}{2}} \pmod{p^3}$

CHRISTIAN AEBI AND GRANT CAIRNS

In geometry, *Morley's miracle* says that in every planar triangle the adjacent angle trisectors meet at the vertices of an equilateral triangle. Frank Morley obtained this wonderful result in 1899, and to this day it continues to attract interest. There are now many known proofs; see the cut-the-knot web site [1]. Perhaps the most celebrated ones are those due to Alain Connes [2] and John Conway (unpublished, yet accessible at [1]). A proof in the same spirit as Connes' was published earlier by Liang-shin Hahn [6]; see also [4]. Conway's proof is perhaps the simplest and nicest one; a somewhat longer proof having the same general approach was given by Coxeter [3], and attributed to Raoul Bricard; see also [10, 12].



Morley's miracle was by no means his sole surprising discovery. In number theory, he published the following result in the *Annals of Mathematics* 1894/95.

Morley's Congruence [9]. *If p is prime and $p > 3$, then*

$$(-1)^{(p-1)/2} \cdot \binom{p-1}{\frac{p-1}{2}} \equiv 2^{2p-2} \pmod{p^3}.$$

To appreciate the “miraculous” nature of this congruence, one first needs to compare it with other congruences known at the time. Some famous ones for primes p include:

- Fermat's little theorem: $2^{p-1} \equiv 1 \pmod{p}$.
- Wilson's theorem: $(p-1)! \equiv -1 \pmod{p}$.
- Lucas' theorem: If $0 \leq n, j < p$, then $\binom{pm+n}{pi+j} \equiv \binom{m}{i} \binom{n}{j} \pmod{p}$.

The above three congruences are modulo p , while Morley's congruence is modulo p^3 . The difference between mod p^3 and mod p is analogous to having a result to three significant figures, rather than just one significant figure.

The other striking aspect of Morley's congruence was the nature of his original proof, which made an ingenious use of integration of trigonometric sums. First he used the

Fourier series:

$$2^{2n} \cos^{2n+1} x = \cos(2n+1)x + (2n+1) \cos(2n-1)x + \frac{(2n+1)2n}{1 \cdot 2} \cos(2n-3)x \\ + \cdots + \frac{(2n+1)2n \cdots (n+2)}{n!} \cos x.$$

He integrated this term by term and compared it with the following formula, which can be obtained by induction using integration by parts:

$$(1) \quad \int_0^{\frac{1}{2}\pi} \cos^{2n+1} x dx = \frac{2n(2n-2) \cdots 2}{(2n+1)(2n-1) \cdots 3}.$$

This established his result modulo p^2 , where $p = 2n+1$. To obtain the result modulo p^3 , Morley then used (1) again to integrate the following power series in $\cos(x)$, known from “treatises on trigonometry”:

$$(-1)^{\frac{p-1}{2}} \cos px = p \cos x - \frac{p(p^2-1^2)}{3!} \cos^3 x + \frac{p(p^2-1^2)(p^2-3^2)}{5!} \cos^5 x \\ - \cdots + (-1)^{\frac{p-1}{2}} 2^{p-1} \cos^p x.$$

Subsequently, two alternate proofs were given that used the properties of Bernoulli numbers: the 1913 Royal Danish Academy of Sciences paper by Niels Nielsen [11, p. 353] and the 1938 Annals of Mathematics paper by Emma Lehmer [8, p. 360].

The main aim of this note is to establish Morley’s congruence by entirely elementary number theory arguments. The key to this approach is the following basic congruence modulo p that curiously, we have not seen in the literature.

Lemma 1. *If p is prime and $p > 3$, then $\sum_{\substack{0 < i < j < p \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij} \equiv 0 \pmod{p}$.*

Here, $\frac{1}{ij}$ denotes the multiplicative inverse of ij modulo p . Throughout this note, p is a prime greater than 3 and by a slight abuse of notation, $\frac{1}{i}$ will denote the fraction $1/i$ or the multiplicative inverse of i modulo p or modulo p^2 , according to the context.

After we have established Morley’s congruence, we will show in the final section that it can also be deduced from Granville’s elegant proof of Skula’s conjecture [5].

REDUCTION OF THE PROBLEM

We will use the following well known facts [7, Theorem 117], that we prove for completeness.

Lemma 2. (a) $\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i^2} \equiv 0 \pmod{p}$, (b) $\sum_{i=1}^{p-1} \frac{(-1)^i}{i} \equiv \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i} \pmod{p^2}$.

Proof. (a) As $\frac{1}{i^2} \equiv \frac{1}{(p-i)^2} \pmod{p}$, one has

$$2 \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i^2} = \sum_{i=1}^p \frac{1}{i^2} = \sum_{i=1}^p i^{-2} = \frac{(p-1)p(2p-1)}{6} \equiv 0 \pmod{p}.$$

(b) For all $0 < i \leq \frac{p-1}{2}$, one has $i(p-i) + i^2 \equiv -p(p-i) \pmod{p^2}$ and dividing by $i^2(p-i)$ gives $\frac{1}{i} + \frac{1}{p-i} \equiv -\frac{p}{i^2} \pmod{p^2}$. Summing and using (a) gives $\sum_{i=1}^{p-1} \frac{1}{i} \equiv 0 \pmod{p^2}$, which is known as Wolstenholme's theorem. Thus

$$\sum_{i=1}^{p-1} \frac{(-1)^i}{i} \equiv 2 \sum_{\substack{i=2 \\ i \text{ even}}}^{p-1} \frac{1}{i} \equiv \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i} \pmod{p^2}.$$

□

Turning to the terms in Morley's congruence, first note that

$$\binom{p}{i} = \frac{p \cdot (p-1) \cdot (p-2) \cdots (p-(i-1))}{i \cdot 1 \cdot 2 \cdots (i-1)}$$

and so

$$(2) \quad \binom{p}{i} = (-1)^{i-1} \cdot \frac{p}{i} \cdot \left(1 - \frac{p}{1}\right) \cdot \left(1 - \frac{p}{2}\right) \cdots \left(1 - \frac{p}{i-1}\right).$$

Thus $\binom{p}{i} \equiv (-1)^i \cdot \left(-\frac{p}{i} + p^2 \cdot \sum_{j=1}^{i-1} \frac{1}{ij}\right) \pmod{p^3}$ and so $2^p = 2 + \sum_{i=1}^{p-1} \binom{p}{i}$ gives

$$2^{p-1} \equiv 1 - \frac{p}{2} \cdot \sum_{i=1}^{p-1} \frac{(-1)^i}{i} + \frac{p^2}{2} \cdot \sum_{0 < j < i < p} \frac{(-1)^i}{ij} \pmod{p^3}.$$

Squaring, and using Lemma 2(b), we have

$$(3) \quad 2^{2p-2} \equiv 1 - p \cdot \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i} + p^2 \cdot \left(\frac{1}{4} \left(\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i} \right)^2 + \sum_{0 < j < i < p} \frac{(-1)^i}{ij} \right) \pmod{p^3}.$$

From (2) we also have $(-1)^{i-1} \binom{p-1}{i-1} = (-1)^{i-1} \frac{i}{p} \binom{p}{i} = \left(1 - \frac{p}{1}\right) \cdot \left(1 - \frac{p}{2}\right) \cdots \left(1 - \frac{p}{i-1}\right)$. Taking $i = \frac{p+1}{2}$ gives $(-1)^{\frac{p-1}{2}} \cdot \binom{p-1}{\frac{p-1}{2}} \equiv 1 - p \cdot \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i} + p^2 \cdot \sum_{1 \leq j < i \leq \frac{p-1}{2}} \frac{1}{ij} \pmod{p^3}$, or equivalently, using Lemma 2(a),

$$(4) \quad (-1)^{\frac{p-1}{2}} \cdot \binom{p-1}{\frac{p-1}{2}} \equiv 1 - p \cdot \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i} + \frac{p^2}{2} \cdot \left(\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i} \right)^2 \pmod{p^3}.$$

Comparing (3) and (4), we observe that Morley's congruence is therefore valid mod p^2 . In order to obtain it mod p^3 , it suffices to prove that $\frac{1}{4} \left(\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i} \right)^2 \equiv \sum_{0 < j < i < p} \frac{(-1)^i}{ij} \pmod{p}$, or equivalently,

$$(5) \quad \left(\sum_{\substack{0 < i < p \\ i \text{ even}}} \frac{1}{i} \right)^2 \equiv \sum_{0 < j < i < p} \frac{(-1)^i}{ij} \pmod{p}.$$

The considerations so far have reduced Morley's congruence modulo p^3 to a congruence modulo p .

COMPLETION OF THE PROOF

In the remainder of this note, all congruences are taken modulo p . First notice that as $\sum_{\substack{0 < i < p \\ i \text{ even}}} \frac{1}{i} = - \sum_{\substack{0 < i < p \\ i \text{ odd}}} \frac{1}{i}$, the left hand side of (5) is

$$\left(\sum_{\substack{0 < i < p \\ i \text{ even}}} \frac{1}{i} \right)^2 \equiv - \left(\sum_{\substack{0 < i < p \\ i \text{ odd}}} \frac{1}{i} \right) \left(\sum_{\substack{0 < j < p \\ j \text{ even}}} \frac{1}{j} \right) \equiv - \sum_{\substack{0 < j < i < p \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij} - \sum_{\substack{0 < i < j < p \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij}.$$

On the other hand,

$$\sum_{\substack{0 < j < i < p \\ i, j \text{ odd}}} \frac{1}{ij} = \sum_{\substack{0 < i < j < p \\ i, j \text{ even}}} \frac{1}{(p-i)(p-j)} \equiv \sum_{\substack{0 < i < j < p \\ i, j \text{ even}}} \frac{1}{ij}$$

and so the right hand side of (5) is

$$\begin{aligned} \sum_{0 < j < i < p} \frac{(-1)^i}{ij} &= \sum_{\substack{0 < j < i < p \\ i, j \text{ even}}} \frac{1}{ij} - \sum_{\substack{0 < j < i < p \\ i, j \text{ odd}}} \frac{1}{ij} - \sum_{\substack{0 < j < i < p \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij} + \sum_{\substack{0 < j < i < p \\ i \text{ even}, j \text{ odd}}} \frac{1}{ij} \\ &\equiv - \sum_{\substack{0 < j < i < p \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij} + \sum_{\substack{0 < i < j < p \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij}. \end{aligned}$$

Hence (5) follows from Lemma 1, and so the proof of Lemma 1 is our final task.

Proof of Lemma 1. We have

$$\begin{aligned} 2 \sum_{\substack{0 < i < j < p \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij} &= \sum_{\substack{0 < i < j < p \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij} + \frac{1}{(j-i)j} = \sum_{\substack{0 < i < j < p \\ i \text{ odd}, j \text{ even}}} \frac{1}{i(j-i)} = \sum_{\substack{0 < i, k < p \\ i+k < p \\ i, k \text{ odd}}} \frac{1}{ik} \\ &\equiv \sum_{\substack{0 < i < j < p \\ i \text{ odd}, j \text{ even}}} \frac{1}{i(p-j)} \equiv - \sum_{\substack{0 < i < j < p \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij} \end{aligned}$$

which gives the required result, as $p > 3$. □

THE CONNECTION WITH SKULA'S CONJECTURE

Consider the Fermat quotient $q = \frac{2^{p-1}-1}{p}$, and note that

$$(6) \quad 2^{2p-2} = 1 + 2qp + q^2p^2.$$

Adopting the notation of [5], set

$$q(x) = \frac{x^p - (x-1)^p - 1}{p}, \quad g(x) = \sum_{i=1}^{p-1} \frac{x^i}{i}, \quad G(x) = \sum_{i=1}^{p-1} \frac{x^i}{i^2}.$$

Note that $q = q(2)/2$. The following remarkable identity was established in [5]:

$$(7) \quad -G(x) \equiv \frac{1}{p}(q(x) + g(1-x)) \pmod{p},$$

from which Granville deduced Skula's conjecture: $q^2 \equiv -G(2) \pmod{p}$. From (7),

$$2q \equiv -g(-1) - G(2)p \equiv -g(-1) + q^2p \pmod{p^2}.$$

Hence, substituting in (6), we obtain

$$(8) \quad 2^{2p-2} = 1 + 2qp + q^2p^2 \equiv 1 - g(-1)p + \frac{1}{2}g(-1)^2p^2 \pmod{p^3}.$$

From Lemma 2(b), $g(-1) \equiv \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i} \pmod{p^2}$, and so from (8)

$$2^{2p-2} \equiv 1 - \left(\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i} \right) p + \frac{1}{2} \left(\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i} \right)^2 p^2 \pmod{p^3}.$$

Together with (4), this gives Morley's congruence once again.

Acknowledgements. We would like to thank the anonymous referees who proposed both constructive and illuminating remarks.

REFERENCES

1. Alexander Bogomolny, *Cut the knot*, <http://www.cut-the-knot.org/triangle/Morley/>.
2. Alain Connes, *A new proof of Morley's theorem*, Les relations entre les mathématiques et la physique théorique, Inst. Hautes Études Sci., Bures, 1998, pp. 43–46.
3. H. S. M. Coxeter, *Introduction to geometry*, Wiley Classics Library, John Wiley & Sons Inc., New York, 1989, Reprint of the 1969 edition.
4. Hansjörg Geiges, *Beweis des Satzes von Morley nach A. Connes*, Elem. Math. **56** (2001), no. 4, 137–142.
5. Andrew Granville, *The square of the Fermat quotient*, Integers **4** (2004), A22, 3 pp. (electronic).
6. Liang-shin Hahn, *Complex numbers and geometry*, MAA Spectrum, Mathematical Association of America, Washington, DC, 1994.
7. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979.
8. Emma Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. (2) **39** (1938), no. 2, 350–360.
9. F. Morley, *Note on the congruence $2^{4n} \equiv (-1)^n(2n)!/(n!)^2$, where $2n+1$ is a prime*, Ann. of Math. **9** (1894/95), no. 1-6, 168–170.
10. D. J. Newman, *The Morley miracle*, Math. Intelligencer **18** (1996), no. 1, 31–34.
11. Niels Nielsen, *Recherches sur les nombres de Bernoulli*, Danske Vidensk. Selsk. Skr. (7) **10** (1913), 285–366.
12. Gerhard Wanner, *Elementare Beweise des Satzes von Morley*, Elemente der Mathematik **59** (2004), no. 4, 144–150.

DEPARTMENT OF MATHEMATICS, LA TROBE UNIVERSITY, MELBOURNE, AUSTRALIA 3086
E-mail address: G.Cairns@latrobe.edu.au